The Honorable Richard A. Jones

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

LAURA KROTTNER and ISHAYA SHAMASA, individually and on behalf of all others similarly situated, Plaintiffs, v. STARBUCKS CORPORATION, a Washington Corporation, Defendant.	No. C09-00216 (RAJ) AMENDED CLASS ACTION COMPLAINT JURY TRIAL DEMANDED

I. INTRODUCTION

Plaintiffs Laura Krottner and Ishaya Shamasa ("Plaintiffs"), individually and on behalf of all others similarly situated, allege the following against Starbucks Corporation ("Defendant" or "Starbucks"), based upon personal knowledge, where applicable, and on information and belief, and the investigation and research of counsel.

II. NATURE OF THE ACTION

1. Plaintiffs bring this class action suit on their own behalf, and on behalf of all entities and persons similarly situated, against Starbucks, as a result of its failure to adequately

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

safeguard its employees' sensitive, personal information, including social security numbers (hereinafter "Personally Identifiable Information" or "PII").

2. As a result of Starbucks' failure to adequately protect and secure Plaintiffs' and proposed Class Members' PII, unauthorized individuals stole a laptop containing Plaintiffs' and the proposed Class Members' PII (hereinafter the "Breach"). The PII stolen during the Breach contained the names, addresses, and social security numbers of approximately 97,000 Starbucks employees. Plaintiffs and the proposed Class Members were required to provide their PII to Starbucks as part of the employment relationship.

3. This is not the first occasion on which Starbucks has failed to safeguard the PII of its employees. In 2006, Starbucks lost the PII of roughly 60,000 employees. This PII was stored on two laptops that were misplaced by or stolen from Starbucks. Upon information and belief, the PII, which included names and social security numbers, was not encrypted or similarly protected.

4. Prior to the 2006 incident involving the loss of 60,000 employees' PII, Starbucks was the subject of an identity theft ring that included Starbucks' own employee. In 2006, My Tran, a Human Resources Employee at Starbucks who accessed a computer system to steal employee information, was sentenced to 42 months in prison and five years of supervision for her involvement in accessing PII from Starbucks and providing it to members of the identity theft ring. Press Release, U.S. Dept. of Justice, Sept. 27, 2006, *available at* http://www.atg.wa.gov/uploadedFiles/Another/News/Press_Releases/2006/IDTheft-Priorities.pdf (last visited Apr. 28, 2009).

5. As Chief Judge Lasnik observed when sentencing one of the perpetrators in the theft ring, "identity theft can create huge emotional problems for people. We often think of bank

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

fraud as just against a bank or just money, but it damages real people." Press Release, United States Attorney's Office, Western District of Washington, Member of ID Theft Ring That Preyed on Starbucks' Employees Sentenced to Prison (June 2, 2006), *available at* http://www.usdoj.gov/usao/waw/press/2006/jun/nguyen.htm (last visited Apr. 28, 2009). Chief Judge Lasnik also noted that the damage of identity theft isn't just financial, "it causes rifts between husbands and wives, it causes divorces." *Id.*

6. In this electronic age, it is standard practice to encrypt sensitive personal and financial information, such as the PII of employees, to protect such information from both internal and external threats. Defendant's failure to maintain reasonable and adequate security procedures to protect against the theft of Plaintiffs' and the proposed Class Members' PII has put Plaintiffs and the proposed Class Members at an increased and imminent risk of becoming victims of identity theft crimes, fraud, and abuse. In addition, Plaintiffs and the proposed Class have spent and will need to spend considerable time and money to protect themselves as a result of Defendant's conduct.

7. Plaintiffs and the proposed Class will suffer irreversible damage if and when their PII becomes misused. As a proximate result of the Breach, tens of thousands of Starbucks employees, including Plaintiffs, have had their PII compromised, have had their privacy invaded, have been deprived of the exclusive use and control of their PII, have incurred out-of-pocket costs, have lost time, and have otherwise suffered economic damages to consistently monitor their credit card accounts, credit reports, and other financial information to protect their PII from imminent misuse.

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

III. JURISDICTION AND VENUE

8. The Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because Plaintiffs are of diverse citizenship from Defendant; there are more than 100 Class Members nationwide; and the aggregate amount in controversy exceeds $5,000,000, excluding interest and costs.

9. The Court has personal jurisdiction over the parties because Defendant conducts substantial business in this state, has systematic and continuous contacts with this state, and has agents and representatives that can be found in this state.

10. Venue is appropriate under the authority of 28 U.S.C. § 1391(a) because the Defendant resides in this District and/or a substantial part of the challenged actions took place and/or emanated from this District.

IV. CHOICE OF LAW

11. The most significant events and relationships relating to Plaintiffs' Complaint occurred or are found in Washington.

12. The PII and laptop containing the PII were located in Seattle, Washington.

13. The theft of the laptop occurred in Washington.

14. Starbucks is headquartered in Seattle, Washington, and transacts substantial business within the state.

15. The policies forming the contractual basis of Starbucks' obligation to protect Plaintiffs' and the proposed Class's PII were developed in Seattle, Washington.

16. Washington law should apply because the most significant contacts with regard to Plaintiffs' Complaint are tied to Washington.

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

V. PARTIES

17. Plaintiff Laura Krottner is a resident of Chicago, Illinois. She has been a Starbucks employee for three years and received notice from Defendant that her PII may have been breached. She is also a customer of Starbucks.

18. Plaintiff Ishaya Shamasa is a resident of Niles, Illinois, and is a citizen of the State of Illinois. He was a Starbucks employee from August 2005 to September 2008 and received notice from Defendant that his PII may have been breached. He is also a customer of Starbucks

19. Defendant Starbucks is the world's leading roaster and retailer of specialty coffee, and is incorporated and headquartered in the State of Washington. Starbucks' corporate address is 2401 Utah Avenue South, Seattle, Washington 98134. At the fiscal end of 2008, Starbucks operated 7,463 locations worldwide, with 4,329 of those locations operating in the United States. Starbucks employs approximately 176,000 people worldwide. In the United States, Starbucks employs approximately 143,000 people, with 136,000 in company-operated retail stores. Other Starbucks employees work in the company's administrative and regional offices, store development, roasting and warehousing operations. Approximately 33,000 employees are employed outside of the United States, with 32,000 in company-operated retail stores. The remaining employees work in the company's regional support facilities and roasting and warehousing operations.

VI. FACTUAL ALLEGATIONS

20. On or about October 29, 2008, a Starbucks laptop containing the PII of approximately 97,000 Starbucks employees was stolen.

21. The stolen PII contained names, addresses, and social security numbers.

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

22. Upon information and belief, the PII data was unencrypted.

23. Upon information and belief, the theft occurred in the greater Seattle, Washington area, not on Starbucks' premises.

A. Disclosure of the Data Breach

24. More than twenty days after the theft, in a letter dated November 19, 2008, Starbucks informed at least some of those affected that their PII had been stolen. Russell Walker, Vice President of Enterprise Security for Starbucks Coffee Company signed the letter. (hereinafter "Notice Letter") (attached hereto as Exhibit A). The Notice Letter stated that Starbucks Enterprise Security learned that a laptop containing employee information was stolen on October 29, 2008, and that Plaintiffs' PII was compromised in the theft of the laptop.

25. On November 17, 2008, Russell Walker sent a letter on behalf of Starbucks to the Maryland Office of the Attorney General, indicating that the PII of 1,501 Maryland residents had been lost due to the theft of the unencrypted data stored on the laptop.

26. The next day, Mr. Walker sent similar letters to the Attorneys General of Virginia and Maine, and the Executive Director of Hawaii's Department of Commerce and Consumer Affairs, notifying them of the theft of the laptop, the loss of the PII, and the approximate number of victims in each state.

27. The Notice Letter states that Starbucks filed a police report with the Seattle Police Department. Despite substantial effort, Plaintiffs' counsel has not located any record of any report filed with the Seattle Police Department regarding the theft.

28. Starbucks has not provided any further information about the theft or efforts to recover the stolen laptop or PII. Upon information and belief, Starbucks has made no further efforts to recover the lost PII.

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

29. The notification Starbucks sent to its employees was vague and untimely.

B. Plaintiffs' Actions After Receiving the Notice Letter

1. Plaintiff Krottner

30. Prior to having received the Notice Letter, Plaintiff Krottner had never signed up for any credit monitoring services. Shortly after receiving the Notice Letter from Starbucks, Plaintiff Krottner signed up for the one year of Credit Watch Service offered by Starbucks, through Experian. A week or so after receiving the letter, Plaintiff Krottner called her bank and asked them to monitor her bank accounts for suspicious activity.

31. As a result of the Starbucks data Breach, it will be necessary for Plaintiff Krottner to closely monitor her personal accounts. Since receiving the Notice Letter, Plaintiff Krottner has been extra vigilant about watching her banking and 401(k) accounts. She checks these accounts nearly every day and spends a substantial amount of time doing so. Prior to receiving the Notice Letter, Plaintiff Krottner only checked her bank account on a bi-weekly basis, and then only to ensure that her bi-weekly paycheck had been properly deposited.

32. Furthermore, upon the expiration of the one year of credit monitoring offered by Starbucks, Plaintiff Krottner will have to pay out-of-pocket for credit monitoring services she did not otherwise use or need prior to the Breach.

2. Plaintiff Shamasa

33. On November 26, 2008, after receiving notice from Starbucks of the October 2008 Breach of Personally Identifying Information, Plaintiff Shamasa signed up for the Equifax credit monitoring program that Starbucks offered. Each month, Equifax sends Plaintiff Shamasa an email update of any suspicious activity on his credit report. Prior to receiving the Notice Letter, Plaintiff Shamasa had not signed up for any credit monitoring.

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

34. In December 2008, Chase Bank contacted Plaintiff Shamasa to inquire whether he had received checks for his new checking account. However, Plaintiff Shamasa was unaware of the new checking account. Chase Bank explained that there was an attempt to open up a new checking account with his social security number. Plaintiff Shamasa informed Chase Bank that he did not open this new checking account. Chase Bank worked with Plaintiff Shamasa to close the unauthorized account. The Equifax credit monitoring program never notified Plaintiff Shamasa of the unauthorized Chase Bank account opening. In fact, Equifax reported to Plaintiff Shamasa that there had been no suspicious activity on his credit report that month. Equifax Letter to Shamasa, Dec. 1, 2008, attached hereto as Exhibit B.

35. To his knowledge, Plaintiff Shamasa had not suffered any incidents of identity theft prior to the Starbucks Breach. Plaintiff Shamasa is unaware of his PII being involved in a data breach other than the Starbucks Breach. The PII that was contained on the stolen laptop is the same kind needed to open a new checking account at Chase Bank. To his knowledge, Plaintiff Shamasa has never transmitted his social security number over the Internet.

C. Starbucks Has Previously Acted Negligently With Employees' PII

36. Starbucks has a history of inadequately protecting employees' PII. In 2006, Starbucks lost four laptops at its headquarters, two of which contained the PII (names, addresses, and social security numbers) of 50,000 former and 10,000 then-current employees.

37. As was the case in the October 2008 laptop theft, the public report of the lost PII was untimely. The disappearance of the laptops in 2006 was not reported to the public until November 4, 2006, nearly two full months after the computers were known to be missing on September 6, 2006.

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

38. In its notice to employees regarding the 2006 PII breach, Starbucks stated that it was "currently reinforcing our corporate policies and updating procedures related to the protection of personal data in an effort to ensure that this type of incident does not occur in the future." Starbucks Corporation, Press Release, http://www.starbucks.com/aboutus/pressdesc.asp?id=720 (Nov. 3, 2006) (hereinafter referred to as "2006 Notice Letter").

39. As the October 2008 Breach made clear, despite this statement recognizing its inadequate security measures, Starbucks had failed to take appropriate remedial action to safeguard PII. Not only has Starbucks failed to safeguard its laptops securely, it has continued to keep PII in an unencrypted format on its laptops. These failures should have been remediated prior to the October 2008 laptop theft.

40. According to *The Seattle Times*, at the time of the 2006 loss, Starbucks had a policy forbidding the storing of sensitive information, such as social security numbers, on mobile equipment. *See* Melissa Allison, *Starbucks laptop with employee data missing*, The Seattle Times, Nov. 4, 2006, *available at* http://seattletimes.nwsource.com/html/retailreport/2008430880_retailreportdige25lap.html. Thus, in violation of its own policy, Starbucks stored PII on the laptops that were stolen and/or lost in 2006.

41. As a predicate to the October 2008 Breach, Starbucks again violated its own supposed policies by storing Plaintiffs' and the proposed Class's PII on a laptop, which was subsequently stolen.

42. Moreover, Starbucks failed to encrypt this PII, which, as discussed *infra*, is standard business practice.

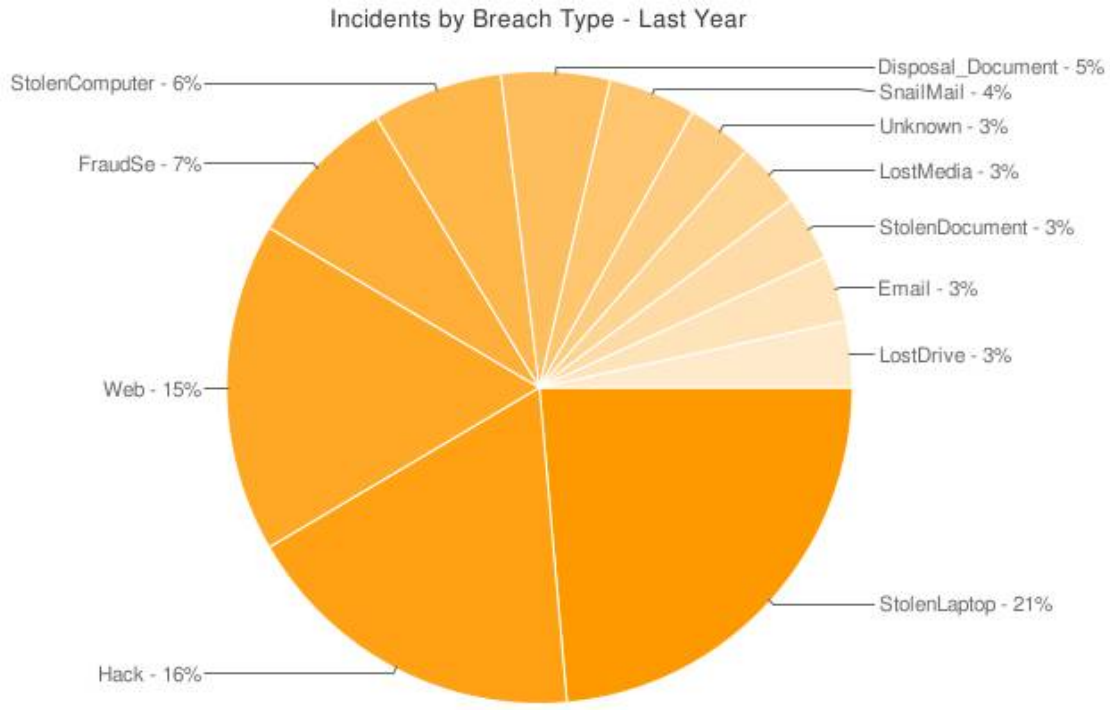
43. Starbucks has subsequently admitted the need for encryption when it notified its employees of the October 2008 Breach: "When these incidents occur, we take the opportunity to

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

once again review our procedures for protecting data and educate our partners about ways to further protect their personal information. We also continue our work to prevent future incidents from occurring. In fact, we are currently implementing encryption solutions where appropriate." *See* Notice Letter.

D. Standard Business Practices for Ensuring Information Safety

44. According to Open Security Foundation's Data Loss DB, the leading source of data theft in 2008 was stolen laptops (21%). Open Security Foundation, *Data Loss Statistics*, http://datalossdb.org/ statistics?timeframe=last_year (last visited Apr. 28, 2009).



45. Federal and state legislatures have passed a number of laws in recent years to ensure that companies protect the security of PII in their possession or control. These laws impose obligations on companies to maintain reasonable security measures to protect the PII of individuals.

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

46. The Federal Trade Commission ("FTC") has issued a publication entitled "Protecting Personal Information: A Guide for Business" ("FTC Report"), attached hereto as Exhibit C. In this publication, the FTC provides guidelines for businesses on how to develop a "sound data security plan" to protect against crimes of identity theft. To protect the personal sensitive information in their files, the FTC Report instructs businesses to follow the following guidelines:

(a) Keep inventory of all computers and laptops where the company stores sensitive data;
(b) Do not collect PII if there is no legitimate business need. If there is a legitimate business need, only keep the information as long as necessary;
(c) Use social security numbers only for required and lawful purposes and do not store these numbers unnecessarily, such as for an employee or customer identification number;
(d) Encrypt the PII, particularly if the sensitive information is shipped to outside carriers or contractors. In addition, the business should keep an inventory of all the information it ships;
(e) Do not store sensitive computer data on any computer with an Internet connection unless it is essential for conducting the business;
(f) Control access to sensitive information by requiring that employees use "strong" passwords; tech security experts believe the longer the password, the better; and
(g) Implement information disposal practices that are reasonable and appropriate to prevent unauthorized access to personally identifying information.

47. In addition, the FTC Report states a number of guidelines concerning the use of laptops in storing PII. As the FTC Report states:

(h) Restrict the use of laptops to employees who need them to perform their jobs;
(i) Assess whether sensitive PII needs to be stored on a laptop, and if not, delete the information with a "wiping" program overwriting the data on the laptop;
(j) Consider allowing laptop users only to access sensitive information but not to store the information on their laptops;
(k) Require employees to store laptops in a secure place; and

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

(l) Encrypt any sensitive data contained on a laptop and configure the data so users cannot download any software or change security settings without approval from Information Technology specialists.

48. The FTC Report also instructs companies that outsource any business functions to investigate the data security practices of any company they outsource business to and to examine those standards.

49. The Washington State Office of the Attorney General in its Consumer Privacy and Data Protection Report also provides a compilation of "best practices" for protecting the personal information collected by businesses. Among those "best practices":

(a) Maintain logs to properly track information and assure that data is only accessed by authorized individuals;
(b) Provide adequate training for employees, agents, and contractors;
(c) Store the information in a secure environment (using features such as doors, locks, firewalls and/or electronic security);
(d) Take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration, and destruction;
(e) Contain consequences for those who fail to comply with the guidelines; and
(f) Participate in privacy seal programs and adhere to the requirements and consequences set forth by such programs.

Paula Selis, Anita Ramasastry, Susan Kim, Cameron Smith, *Consumer Privacy and Data Protection*, Washington State Office of the Attorney General, available at http://www.atg.wa.gov/uploadedFiles/Home/News/Press_Releases/2002/PrivacyPolicy1.doc (last visited Apr. 28, 2009) (hereinafter "Wash. AG Report") (attached hereto as Exhibit D).

50. As a company based in the State of Washington, Starbucks knew or should have known of the Washington State Office of the Attorney General and its Consumer Privacy and Data Protection Report.

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

E. Starbucks Breached Its Common Law Duty To Safeguard Plaintiffs' PII

1. Starbucks Has a Duty to Protect Its Employees' PII

51. Starbucks has a duty to protect its employees' PII.

52. Employees' PII includes sensitive, personal information, such as their names and social security numbers. Such information is a property interest owned by employees and is not owned by Starbucks.

53. As a matter of practice, employers are also obligated to act with the care, skill, prudence, and diligence under the circumstances then prevailing that a prudent person acting in a like capacity and familiar with such matters would use in the conduct of an enterprise of a like character and with like aims.

54. Employees trust Starbucks to protect their PII for the limited purpose of working for the company. Employees expect that their PII will not be disclosed except in the course of managing their employment.

2. Starbucks Breached Its Duty to Protect Its Employees' PII

55. Starbucks failed to fulfill its duty to follow reasonable precautions to secure its employees' PII.

56. Contrary to the best practices propounded by the FTC and Washington's Attorney General, Starbucks did not encrypt the PII it gathered and left on the laptop that was stolen in October 2008.

57. Starbucks also breached its promise to safeguard employee PII, which is memorialized in its Staffing Services Brochure, attached as Exhibit E.

58. Starbucks also failed to provide timely notice of its failure to safeguard employee PII.

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

59. As of at least November 2006, Starbucks knew or should have known to employ adequate and meaningful measures to protect against loss or theft of PII. Moreover, it knew or should have known to encrypt employee PII. It failed to take such actions.

F. Starbucks Breached Its Implied Contracts To Safeguard Employee PII

1. Starbucks Contractually Agreed to Protect Employee PII

a. Application Contract

60. Starbucks and Plaintiffs entered into an implied contract to safeguard Plaintiffs' PII when Plaintiffs began employment at Starbucks ("Application Contract"). As a condition of employment, Starbucks gathers and uses social security numbers to aid it in hiring, promoting, transferring and reassigning employees. In its Owner Staffing Services Brochure, Starbucks sets forth various, specific terms of the agreement: "In consideration of an application for employment, or a current employee for promotion, transfer, reassignment or retention, Starbucks Coffee Company may inquire into the individual's background. This background inquiry may include, but is not limited to obtaining a consumer credit report and/or an investigative consumer credit report for the purposes of validation of a social security number . . . ." Ex. D at 1. According to the Application Contract, Plaintiffs provided their social security numbers to Starbucks with the understanding that Starbucks would safeguard the information.

61. In exchange for this "consideration" from its employees, as part of its Application Contract, Starbucks makes various promises to safeguard its employees' PII. For example, Starbucks states that "[c]onfidential information may be shared on a need-to-know basis," and that access to the information is limited. *Id.* at 2. Implied in this bargain is that Starbucks will protect its employees' PII from disclosure or loss as part of the employment relationship. Thus, Plaintiffs and Starbucks each entered into implied Application Contracts, whereby Plaintiffs

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

would furnish their PII to Starbucks to be considered for employment, and Starbucks, in turn, would safeguard Plaintiffs' information.

b. Partner Privacy Contract

62. Once someone becomes a Starbucks employee, Starbucks also identifies certain standards for maintaining the privacy of its employees in its "Standards of Business Conduct." *See* Starbucks *Standards of Business Conduct*, attached as Exhibit F. The terms of this agreement constitute what will be referred to herein as a "Partner Privacy Contract."

63. In this document, Starbucks lays out the "legal and ethical standards that we all must follow on a day-to-day basis." *Id.* at 3. Under the item "PARTNER PRIVACY AND PERSONAL ACTIVITIES," Starbucks states that "[t]reating each other with respect and dignity includes respecting one another's privacy." *Id.* at 4. Starbucks also states that it "strives to provide a safe work environment for all partners." *Id.* at 5.

64. Of particular note, in its Partner Privacy Contract, Starbucks states in its Standards of Business Conduct regarding "Confidential Materials" that "[j]ust as we take care to protect our information, Starbucks respects the information of others." *Id.* at 15. To this end, Starbucks tells employees:

> DON'T bring any papers or computer records from prior employers to Starbucks;
> DON'T accept or use anyone else's confidential information (or agree to maintain anyone's information in confidence) except under an agreement approved by the Law and Corporate Affairs department;
> DON'T solicit confidential information from another company's present or former employees; and
> DON'T engage in "espionage"; be above board in obtaining information about the marketplace.

Id.

65. Starbucks agreed to protect with equal vigor the PII of its employees. Given that Starbucks and its employees "all must follow [the Standards of Business Conduct] on a day-to-

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

day basis," Starbucks agreed to protect the PII of its employees, including Plaintiffs, just as its employees agreed to protect Starbucks' confidential information.

c. Employee-Customers Contract

66. In yet another privacy contract, Starbucks also represents to its customers, which includes a substantial number of employee-customers, that it will protect their PII ("Employee-Customers Contract"). On its website, Starbucks promises to secure the information that it collects:

> **What type of information does Starbucks collect about me?** Personal Information means information that can be used to identify an individual and includes:
>
> - name, address, phone number, e-mail address, birth date;
> - financial information, such as credit card number;
> - tender loaded on the Starbucks Card through agents such as Coinstar; and
> - employment-related information, such as may be found on resumes, applications, background verification information, or in employment references.
>
> . . .
>
> **How is my personal information secured?** Starbucks strives to maintain appropriate physical, technical and administrative security with respect to its offices and information systems so as to prevent any loss, misuse, unauthorized access, disclosure, or modification of personal information.
>
> We encrypt the pipe through which personal information, such as credit card numbers, is sent, using Secure Socket Layer (SSL) technology to ensure that your information is safe as it is sent over the Internet to our server. . . .

Starbucks Privacy Statement, last modified May 27, 2008, http://www.starbucks.com/customer/privacy.asp (last visited Apr. 28, 2009). Thus, Starbucks encrypts its customers' PII, but has failed to do the same for its employees.

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

2. Starbucks Breached the Contractual Terms

67. By failing to adequately safeguard and protect the laptop that contained PII and that was stolen in October 2008, Starbucks breached the material terms of the implied contracts described *supra*.

68. Starbucks also breached these implied contracts by failing to encrypt its employees' PII. It failed to "respect the information of others." Moreover, Starbucks applied a double standard by encrypting customer PII, while leaving employee PII unencrypted. This conduct violates the letter and spirit of the *quid pro quo* of the Standards of Business Conduct.

G. Consequences of the Breach

69. As a result of Starbuck's negligence and implied breaches of contract, Plaintiffs have suffered damages and the increased risk of future harm and damages. Plaintiffs have spent and continue to expend substantial time to ensure that their identities have not been stolen or used improperly.

70. Moreover, Plaintiffs and the proposed Class stand at a heightened risk of identity theft as a direct and proximate result of the Breach.

71. Data breaches can and do lead to identity theft. The loss of Plaintiffs' PII makes them an easier mark for identity theft because the data lost in a data breach provides an identity thief with a consolidated and verified list of actual PII. In the wrong hands, the probable misdeeds involving Plaintiffs' and the proposed Class Members' PII are limited only by the imagination of the thief.

72. As defined in the Fair and Accurate Credit Transactions Act of 2003, Pub. L. 108-159, Dec. 4, 2003 (FACTA), "identity theft" is a fraud that is committed or attempted when one person is using another person's identifying information without permission. Generally, identity

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

theft occurs when a person's identifying information is used to commit fraud or other crimes. These crimes include credit card fraud, phone or utilities fraud, bank fraud, and government fraud.

73. As the United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report"), more than 570 breaches involving theft of personal identifiers such as social security numbers were reported by the news media from January 2005 through January 2006. See U.S. Gen. Accounting Office, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, June 2007, http://www.gao.gov/news.items/d07737.pdf (last visited Apr. 28, 2009). These data breaches involve the "unauthorized or unintentional exposure, disclosure, or loss of sensitive Confidential Information, which can include personally identifiable information such as Social Security numbers (SSN) or financial information such as credit card numbers." *Id.* at 2.

74. Identity thieves use stolen PII, such as social security numbers, for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank or finance fraud.

75. In a pamphlet called "Identity Theft Repair Kit," the Office of the Attorney General of Colorado, John W. Suthers, outlines the immediate consequences of such a breach. An identity thief can then open a new credit card with the delinquent account reported on the victim's credit report. The imposter changes the mailing address on the victim's credit card account so that it will take some time before the victim realizes that there is a problem. The thief can establish phone or wireless service in the victim's name or open a bank account and use it to write bad checks. The thief can also file for bankruptcy to avoid paying debts or to avoid eviction. If arrested, the thief can give the police the victim's name, affecting their criminal record and subjecting the victim to arrest for not appearing in court. The thief can also make

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

purchases related to illegal activities or take out an auto loan. *See* Colorado Attorney General, *Identity Theft Repair Kit*, http://www.ago.state.co.us/idtheft/idtrk.pdf (last visited Apr. 28, 2009).

76. Identity theft crimes often include more than just crimes of financial loss. Identity thieves also commit various types of government fraud, such as: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and social security number to obtain government benefits; or filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's social security number, rent a house or get medical services in the victim's name, and may even give the victim's PII to police during an arrest resulting in an arrest warrant being issued in the victim's name.

77. Victims of identity theft often have a great deal of difficulty clearing their credit records, which can significantly impair their credit rating and ability to obtain loans. While law enforcement, banks, credit bureaus, and collection agencies all have procedures to help identity theft victims, it can still take weeks, months, or years of effort and frustration to return to normal. A damaged credit history can also cause difficulty for the victim in obtaining a new job or renting an apartment, as employers and landlords often review credit records of new applicants. *Id*.

78. Identity theft victims spend numerous hours and money repairing damage to their good name and credit record. In addition, a person whose PII has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office, which conducted a comprehensive and extensive study of data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

> information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See U.S. Gen. Accounting Office, *Personal Information*, *supra*. Thus, Plaintiffs and the proposed Class Members now face years of constant surveillance and monitoring to prevent further loss and damage.

H. The Inadequate Remedy

79. In the Notice Letter, Starbucks stated that it had "no indication that the private information has been misused." However, Starbucks provided no basis for this conclusion, nor any guarantees that the information would not be misused in the future. In fact, Plaintiff Shamasa has had his identity stolen as a result of the Breach. In December 2008, just 2 months after the Breach, Plaintiff Shamasa learned that someone had used his PII to open a bank account with Chase Bank. Plaintiff Shamasa worked with Chase Bank to close this unauthorized account. The Equifax credit monitoring Plaintiff Shamasa signed up for through Starbucks' offer failed to report or prevent this unauthorized account. Starbucks' proposed remedy was inadequate.

80. Since the Breach, various people have commented on Starbucks-related Internet message boards that they have been victims, or know people who have been victims, of identity theft as a result of the Breach.

81. Now that Starbucks has compromised the putative Class's PII, Plaintiffs and the proposed Class have spent and will continue to spend considerable time and money attempting to prevent and monitoring for fraudulent activity on their financial accounts. According to the Washington State Attorney General's Consumer Privacy and Data Protection Report, "[i]ndividual victims of identity theft spend an average of two or more years attempting to fix their credit report and restore their credit status" Wash. AG Report, Exhibit D, at 5.

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

82. The Notice Letter provided only a limited remedy to Plaintiffs and the proposed Class. The remedy Starbucks offered was credit watch services from Equifax for one year.

83. The credit watch service offered by Starbucks is sold by Equifax as "Equifax Credit Watch™ Silver" (hereinafter "Silver Package").

84. The one year of Silver Package credit watch services offered by Starbucks inadequately protects Plaintiffs and the putative Class from identity theft. Among other reasons, the remedy is inadequate because:

(a) Starbucks has only offered one year of protection;
(b) Starbucks only provides weekly access to credit reports, rather than the daily access that is prudent and available under "Equifax Credit Watch™ Gold";
(c) Starbucks' offer leaves Plaintiffs and the Class responsible for a $250 deductable for any identity theft claims;
(d) The offer fails to compensate Plaintiffs and the Class for their time and resources they have and will have to expend to ensure that their credit records are not misused by the criminals who now have Plaintiffs' and the Class's PII; and
(e) Starbucks does not offer identity restoration, which will make Plaintiffs and the Class whole in case their identity has been stolen.

85. Starbucks' failure to maintain reasonable and adequate security procedures to protect against the theft of their employees' PII has placed Plaintiffs and the other proposed Class Members at an increased risk of becoming victims of identity theft crimes. In addition, Plaintiffs and the proposed Class Members have spent and will need to spend considerable time and money protecting themselves as a result of Defendant's conduct.

86. Due to the fact that Plaintiffs and the proposed Class have had their social security numbers stolen as a result of Defendant's conduct, Plaintiffs and the proposed Class will now have to consistently monitor their credit card accounts, credit reports and other financial information to guard against the harm of the risk to which they have been subjected. Social

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

security numbers are virtually impossible to change. Thus, Plaintiffs and the proposed Class will continue to be at risk for identity theft for the rest of their lives.

87. As a result, Plaintiffs and the proposed Class seek damages, restitution, declaratory relief, injunctive relief, and any other such relief as the Court may award.

VII. CLASS ACTION ALLEGATIONS

88. Plaintiffs bring this suit as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of themselves and all others similarly situated, as members of a Class initially defined as follows:

> All persons whose Personally Identifiable Information was contained on the Starbucks laptop that was stolen or otherwise misplaced on or about October 29, 2008.

89. Numerosity. The proposed Class is sufficiently numerous, as approximately 97,000 Starbucks employees have had their PII compromised. Putative Class Members are so numerous and dispersed throughout the United States that joinder of all members is impracticable. Putative Class Members can be identified by records maintained by Defendant. Plaintiffs allege, upon information and belief, that Defendant has already contacted the approximately 97,000 employees whose PII was compromised when notifying the employees of the Breach.

90. Common Questions of Fact and Law. Common questions of fact and law exist as to all members of the proposed Class and predominate over any questions affecting solely individual members of the proposed Class, pursuant to Rule 23(b)(3). Among the questions of fact and law that predominate over any individual issues are:

(a) Whether Starbucks failed to exercise reasonable care to protect Plaintiffs' and the proposed Class's PII;

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

(b) Whether Starbucks owed a legal duty to Plaintiffs and the proposed Class to protect their PII and whether Defendant breached this duty;
(c) Whether Starbucks was negligent;
(d) Whether Starbucks created a bargained-for promise to protect its employees' PII that is supported by consideration;
(e) Whether Starbucks breached this contractual obligation by failing to protect its employees' PII;
(f) Whether Plaintiffs and the proposed Class are at an increased risk of identity theft as a result of Starbucks' breaches and failure to protect Plaintiffs' and the proposed Class's PII; and
(g) Whether Plaintiffs and members of the proposed Class are entitled to the relief sought, including injunctive relief.

91. Typicality. Plaintiffs' claims are typical of the claims of members of the proposed Class because Plaintiffs and the proposed Class sustained damages arising out of Defendant's wrongful conduct as detailed herein. Specifically, Plaintiffs' and proposed Class Members' claims arise from Starbucks' failure to install and maintain reasonable security measures to protect Plaintiffs' and the proposed Class's PII.

92. Adequacy. Plaintiffs will fairly and adequately protect the interests of proposed Class Members and has retained counsel competent and experienced in class action lawsuits. Plaintiffs have no interests antagonistic to or in conflict with those of proposed Class Members and therefore are adequate representatives for proposed Class Members.

93. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because the joinder of all putative Class Members is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of an inconsistent and potentially conflicting adjudication of the claims asserted herein. There will be no difficulty in the management of this action as a class action.

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

VIII. CAUSES OF ACTION

COUNT I
Negligence

94. Plaintiffs repeat and re-allege the allegations contained in each of the paragraphs of this Complaint as if fully set forth herein.

95. Defendant had a duty to exercise reasonable care to protect and secure Plaintiffs' and the proposed Class Members' PII within its possession or control.

96. Defendant knew or should have known of industry standards and "best practices" of the industry when it came to protecting the private information of its employees and applicants.

97. Defendant failed to make good on its promises to safeguard employee PII after its 2006 loss of PII.

98. Through its acts and omissions described herein, Defendant unlawfully breached its duty to use reasonable care to protect and secure Plaintiffs' and the proposed Class Members' PII within its possession or control. More specifically, Defendant failed to maintain a number of reasonable security procedures and practices designed to protect the PII of Plaintiffs and the Class, including, but not limited to:

(a) Using social security numbers only for necessary, required, and/or lawful uses;
(b) Limiting access to PII to employees with a "need to know";
(c) Encrypting any sensitive data contained on a laptop, computer network, and/or disks, as well as configuring the data so it could not be downloaded to a portable device;
(d) Utilizing an "auto-destroy" function so that data on a computer that is reported stolen will be destroyed when the thief uses the computer;
(e) Refraining from storing PII on a laptop;
(f) Allowing laptop users to access sensitive information but not to store the information on their laptops;
(g) Requiring employees to store laptops in a secure place (using features such as doors, laptop locks, firewalls, and/or electronic security);

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

(h) Providing adequate training for employees, agents, and contractors;
(i) Implementing information disposal practices reasonable and appropriate to prevent unauthorized access to PII;
(j) Participating in privacy seal programs and adhering to the requirements and consequences set forth by such programs;
(k) Imposing disciplinary measures for security policy violations; and
(l) Creating a "culture of security" by implementing a regular schedule of employee training.

99. As a direct and proximate result of Defendant's breach of its duties, Plaintiffs and the proposed Class have been harmed by the release of their PII, causing them to expend personal income on credit monitoring services and putting them at an increased risk of identity theft. Plaintiffs and the proposed Class have spent time and money to protect themselves as a result of Defendant's conduct, and will continue to be required to spend time and money protecting themselves, their credit, and their reputations.

COUNT II
Breach of Implied Contract

100. Plaintiffs repeat and re-allege the allegations contained in each of the paragraphs of this Complaint as if fully set forth herein.

101. Defendant came into possession of Plaintiffs' and the proposed Class Members' PII for the purposes of applying for and maintaining employment with Starbucks, and impliedly contracted with Plaintiffs and proposed Class Members to protect such information. The contractual agreement specified that PII was a necessary item of "consideration" for employment.

102. The terms of the contract, memorialized in Starbucks' Owner Staffing Services Brochure, its Standards of Business Conduct, and its Employee-Customer Privacy Contract,

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

required Defendant to safeguard and protect Plaintiffs' and the proposed Class Members' PII from being breached, compromised, and/or stolen.

103. Defendant did not safeguard or protect Plaintiffs' and the proposed Class Members' PII from being compromised and/or stolen. Defendant failed to provide the level of security it promised to provide to its employees.

104. Because Defendant failed to safeguard and protect Plaintiffs' and the proposed Class Members' PII from being compromised or stolen, Defendant breached its contracts with Plaintiffs and the proposed Class Members.

105. The duties breached by Defendant arise solely out of the terms of the implied contracts alleged *supra*.

106. Plaintiffs and the proposed Class Members suffered and will continue to suffer actual damages, including, but not limited to, the cost and time spent on bank and credit monitoring, identity theft, insurance fraud, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm.

PRAYER FOR RELIEF

A. For an order certifying the proposed Class herein under Federal Rule of Civil Procedure 23(a) and (b)(3) and appointing Plaintiffs and Plaintiffs' counsel of record to represent said proposed Class;

B. Finding that Starbucks breached its duty to safeguard and protect Plaintiffs' and the proposed Class Members' PII stored on Starbucks' laptop that was lost on or about October 29, 2008;

C. Finding that Starbucks breached its contracts with its employees to protect their PII;

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

D. Awarding injunctive relief, including but not limited to: (i) the provision of credit monitoring and/or credit card monitoring services for the proposed Class for at least five years; (ii) the provision of bank monitoring and/or bank monitoring services for the proposed Class for at least five years; (iii) the provision of identity theft insurance for the proposed Class for at least five years; (iv) the provision of credit restoration services for the proposed Class for at least five years; (v) awarding Plaintiffs and the proposed Class Members the reasonable costs and expenses of suit, including attorneys' fees, filing fees, and insurance for the proposed Class; and (vi) requiring that Starbucks receive periodic compliance audits by a third party regarding the security of its computer systems, specifically including laptops, used for processing and storing customer data, to ensure its compliance with federal and industry rules, regulations, and practices;

E. Awarding the damages requested herein to Plaintiffs and the proposed Class;

F. Awarding all costs, including experts' fees and attorneys' fees, and the costs of prosecuting this action;

G. Awarding pre-judgment and post-judgment interest as prescribed by law; and

H. Granting additional legal or equitable relief as this Court may find just and proper.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all issues so triable.

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

DATED this 28th day of April, 2009.

KELLER ROHRBACK L.L.P.

By /s/ Ian J. Mensher

Lynn Lincoln Sarko, WSBA #16569
Mark A. Griffin, WSBA #16296
Gretchen Freeman Cappio, WSBA #29576
Ian J. Mensher, WSBA #39593
1201 Third Avenue, Suite 3200
Seattle, WA 98101-3052
Telephone (206) 623-1900, Fax (206) 623-3384
Email: lsarko@kellerrohrback.com
mgriffin@kellerrohrback.com
gcappio@kellerrohrback.com
imenshere@kellerrohrback.com

FINKELSTEIN THOMPSON LLP
Mila F. Bartos (admitted *pro hac vice*)
Karen J. Marcus (admitted *pro hac vice*)
Eugene J. Benick (admitted *pro hac vice*)
1050 30th Street, NW
Washington, D.C. 20007
Telephone: (202) 337-8000, Fax: (202) 337-8090
Email: mbartos@finkelsteinthompson.com
kmarcus@finkelsteinthompson.com
ebenick@finkelsteinthompson.com

Attorneys for Plaintiffs Krottner and Shamasa and the Proposed Class

CERTIFICATE OF SERVICE

I hereby certify that on April 28, 2009, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which sent notification of such filing to the registered CM/ECF users in this case. There are no non CM/ECF participants.

DATED this 28th day of April, 2009.

/s/Mavis J. Bates
Mavis J. Bates, Legal Assistant

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384